Panagiota Kiourti, PhD

pkiourti@gmail.com | Google Scholar | Linkedin | GitHub | Redwood City, CA

About/Summary

AI / ML Scientist with expertise in AI security and explainability, and experience in computer vision and 3D geometry. Skilled in building ML models, publishing pioneering research on backdoor defenses, and delivering production-ready code that powers high-impact products.

Experience

Carbon3D Redwood City, CA
Senior Software Engineer July 2024-Nov 2025
Research Scientist Intern Summer 2022

- Built ML pipelines that **automatically orients 3D scans/meshes of dentures for 3D printing achieving 99.7% success rate** and enabling a multi-million-dollar revenue stream.
- Leveraged camera calibration to recover 3D tilt across cross-functional teams with production-grade accuracy.
- Implemented NVIDIA's NGLOD (neural level-of-detail for 3D) fast training process in PyTorch, enabling real-time neural implicit (SDF) representation, **achieving 98% compression rate** of large objects.

SRI International Menlo Park, CA
Computer Science Intern Summer 2020
Reinforcement Learning Intern Summer 2019

- **Created backdoor detection** method for image classification NNs (IARPA TROJAI program), **achieving 96% AUC**.
- Extended backdoor attacks in LSTM-based Reinforcement Learning networks with 100%.

Flashchat Athens, Greece
Full-Stack Developer Aug 2017–Apr 2018

- Built AI chatbots for e-commerce; **boosted** efficiency of **customer data workflows** 4×.

Intrasoft International Athens, Greece
Software & Test Engineer Apr 2016–July 2017

- Built UI & automation tests for Lottery Management Software (ReactJS, NodeJS, JIRA).

Projects

- ArXiv Paper Triage (Ollama LLM Summarization) 2025

  App that queries arXiv, clusters titles, and generates structured JSON per paper. (sentence-transformers)

Skills

- **ML/AI**: PyTorch (TorchVision, Lightning, timm); TensorFlow; scikit-learn; NumPy, SciPy; Hugging Face (Transformers, sentence-transformers); ONNX; XAI (Captum, SHAP); OCR (TrOCR)
- **CV/3D**: OpenCV; scikit-image; 3D geometry (Trimesh, PyMeshLab, PyVista, Open3D); Blender API; PointNet, MeshCNN, PointTransformer, Point-clouds & shape completion (FoldingNet, PoinTr, AdaPoinTr); GraphCNN
- **Visualization**: Plotly, Matplotlib; Dash, Streamlit
- **Programming:** Python, C++, Java, JavaScript, (React/Node), Flask, SQL, NoSQL, MongoDB, Bazel
- **Full-Stack Development**, **Cybersecurity**
- **Core Strengths:** Analytical Thinking, Communication, Adaptability, Initiative, Presentation skills

Publications/Media Coverage

- Kiourti Panagiota et al. "Misa: Online defense of trojaned models using misattributions." ACSAC'21.
- Kiourti Panagiota et al. "Trojdrl: evaluation of backdoor attacks on deep reinforcement learning." DAC'20.
  Featured in WIRED magazine:
  Tainted Data Can Teach Algorithms the Wrong Lessons

Teaching

- **Teaching Assistant** at Boston University 2019–2020
  Cybersecurity (EC521), Operating Systems (EC440)

Certifications & Courses

- **Mathematics Behind LLMs & Transformers** Certificate of Completion | Udemy 2025
- **3D Machine Learning with PyTorch3D**
  Certificate of Completion | Educative 2025
- **Neural Radiance Fields (NeRF)**
  Certificate of Completion | Udemy 2025

Education

Boston University Boston, MA
PhD & MSc in Computer Engineering, GPA: 3.91/4.00 Sept 2018–Jun 2024

- Thesis: Enhancing deep learning security through explainability and robustness
- Pioneered first deep reinforcement learning backdoor attack methodology; developed defense strategies.

National Technical University of Athens Athens, Greece
BSc & MEng (*Combined degree*) in Electrical and Computer Engineering, GPA: 7.95/10.0 Sept 2015